Fin Security & Privacy

At Fin, we recognize that our success is deeply tied to your trust in us and our ability to keep the information you share with us secure.

> This document is an overview of the processes we follow and the features available for you to control your data.

Fin has the following security and privacy certifications:

SOC 2 Type 2, ISO 27001, and ISO 27701 certifications.

Fin offers features to help you maintain compliance with:

- HIPAA
- GDPR
- CCPA

Independent, third parties conduct a penetration test once a year and perform an audit of our security practices annually. We also periodically test and audit our code and application to look for potential security issues. Additionally, all code is reviewed by a second engineer before being deployed and all changes are logged.

Information Fin collects

Fin does not require access to the personal data of your customers in order to provide services to you. Any personal data of your customers that you choose to pass on to Fin, and some of the personal data of your employees (referred to herein as "agents"), will be captured in an optional recording feature.

Outside of recordings, the only personal data we collect through metrics are: agent's name, agent's relationship to you (our customer), agent's IP address, and agent's browsing history.

You control your team's access

We enable you to limit the permissions each user in your organization has by assigning them roles based on the kind of data they are allowed to access.

We currently offer four roles:

Member	Viewer
Manager	Admin

Whenever any user accesses a recording on the site, that access is logged. These logs are available to customers upon request.

You can revoke access to users who no longer need it by deleting them. By default, deleted users are "soft-deleted," meaning we expire their sessions and no longer allow them to log in while the data they have already uploaded is still available to you. A user's data can be permanently deleted from the dashboard.

Access to your data is controlled and limited

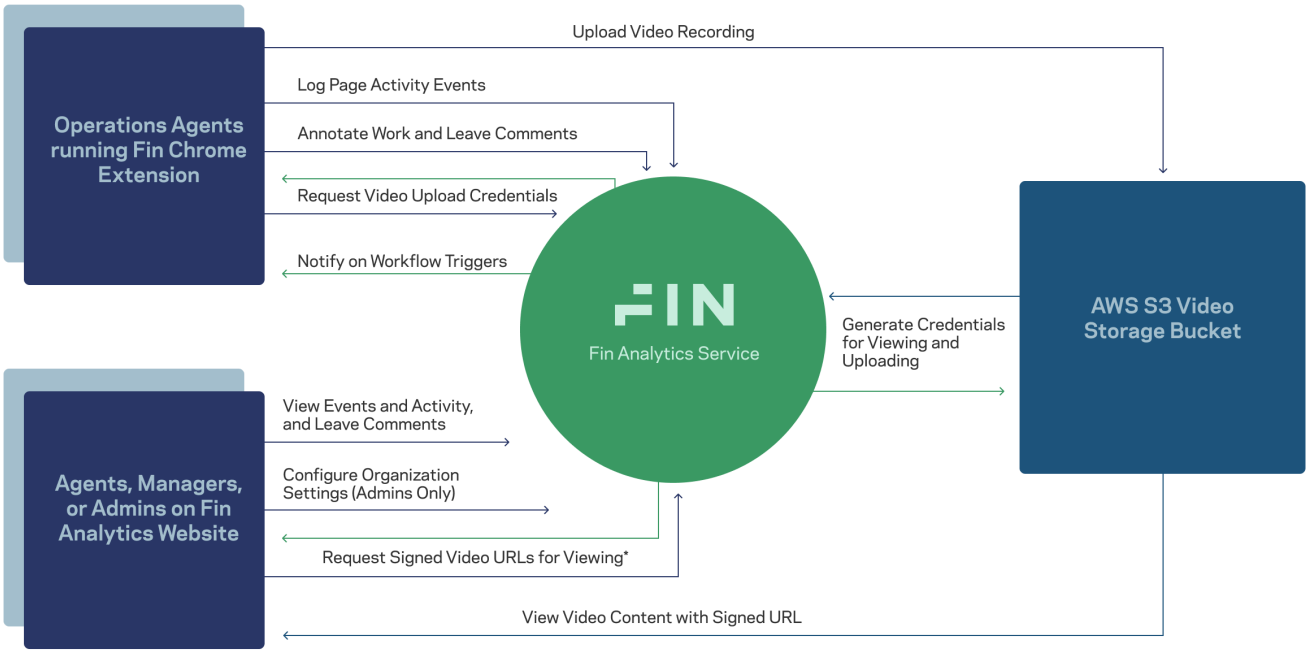
You have control over who can access the recordings. Fin provides access logs (which include an IP address) with information on who has accessed your recordings. You also have control over where the recordings are stored, either in your S3 bucket or ours. Additional features include the ability to require multi-factor authentication as well as automatically redacting video by setting up URL pattern-based blacklists.

Employees at Fin do NOT have the ability to log into our application as your organization or access your audio and video recordings, unless you explicitly create an account to grant us access, such as for troubleshooting instances.

Within our backend systems only select members of the security team have access to the S3 buckets we use to store your recordings. Security team members are prohibited through our policies from accessing your recordings unless explicitly requested by you. In the event a security team member assumes a role with access to recordings, the access is logged and the entire security team is alerted. Other members of the security team review the logs to ensure compliance. Engineers working on the application code use IAM roles that do NOT permit them to access recordings.

Your data is encrypted

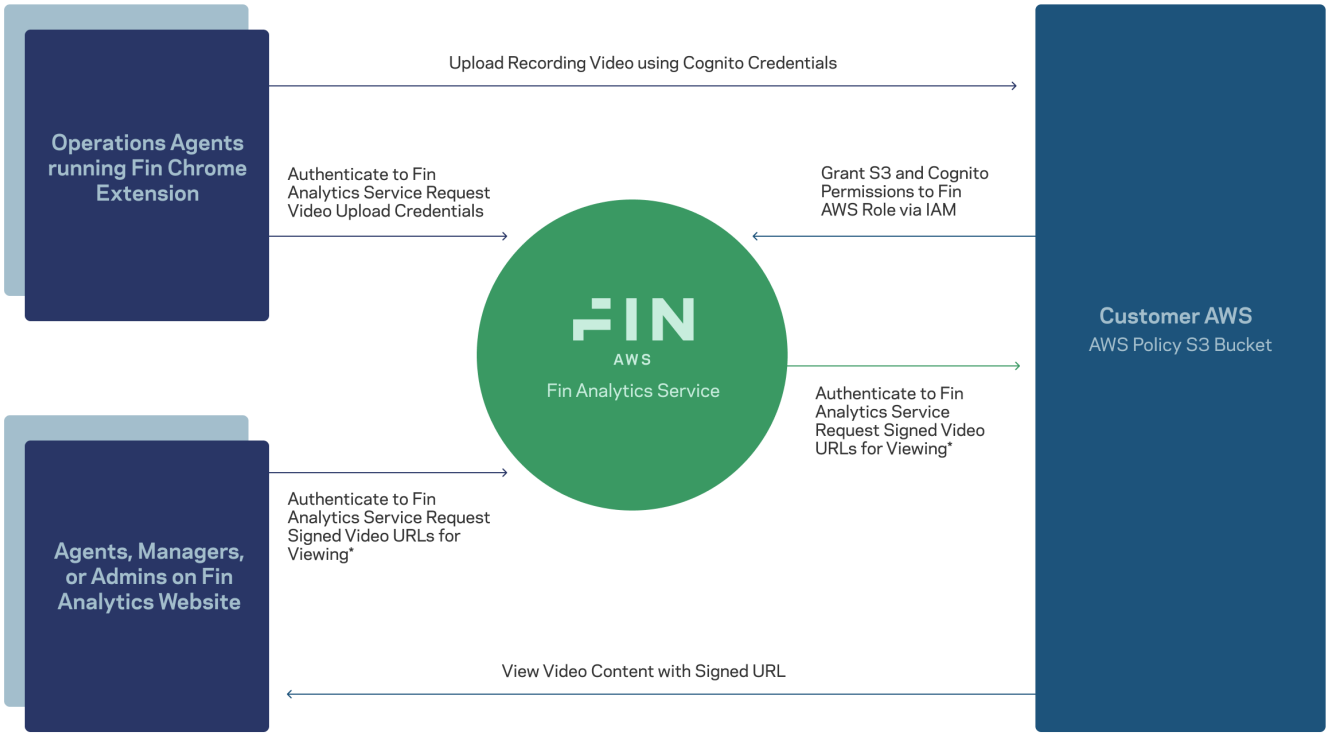
We store the audio and video recordings you share with us on AWS S3. When stored on disk, they are encrypted using industry-standard AES-256 encryption. When they are in transit, we transmit your data over HTTPS using certificates from valid public CAs.



* Depending on permission settings that you can customze, some users will only be granted access to certain videos or non at all.

Store Recordings in Fin's cloud or your own cloud

Although recording data storage with Fin is set up to meet stringent security and privacy requirements, some customers prefer storing video assets in their own AWS environment, which Fin enables. By storing recordings in your own S3 bucket, you have control over who has access to the data, including the Fin web app, and would be able to shut off Fin's access at any time.



* Depending on permission settings that you can customze, some users will only be granted access to certain videos or non at all.

For further Security & Privacy details, please email us at **security@fin.com**.